

We claim:

1. A method of secure communication comprising:

providing a communication implementation between at least first and second

parties;

5 establishing a secure tunnel between the at least first and second parties using an encryption algorithm;

authenticating between the at least first and second parties over the secured

tunnel;

provisioning secure credentials between the at least first and second parties using

10 the secured tunnel.

2. The method of claim 1 wherein the communication implementation between the

at least first and second parties is at least one of a wired implementation and a wireless

implementation.

15

3. The method of claim 1 wherein the encryption algorithm is an asymmetric

encryption algorithm.

4. The method of claim 3 wherein the asymmetric encryption algorithm is used to

20 derive a shared secret, subsequently used in the step of establishing a secure tunnel.

5. The method of claim 3 wherein the asymmetric encryption algorithm is Diffie-

Hellman key exchange.

6. The method of claim 1 wherein the step of authenticating is performed using Microsoft MS-CHAP v2.

5 7. The method of claim 1 further comprising a step of provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties.

8. The method of claim 7 wherein the step of provisioning a public/private key pair
10 comprises providing a server-side certificate in accordance with Public Key Infrastructure (PKI).

9. An implementation for enabling secure communication comprising:
an implementation for enabling communication between first and second parties;
an implementation for establishing a secure tunnel between the at least first and
15 second parties using an encryption algorithm;
an implementation for provisioning secure credentials over the secured tunnel
between the at least first and second parties;
an implementation for authenticating between the at least first and second parties
over the secured tunnel.

20 10. The implementation of claim 9 wherein the implementation for enabling communication between first and second parties is at least one of a wired implementation and a wireless implementation.

11. The implementation of claim 9 wherein the encryption algorithm is an asymmetric encryption algorithm.

5 12. The implementation of claim 11 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.

13. The implementation of claim 11 wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange.

10

14. The implementation of claim 9 wherein the implementation for authenticating comprises Microsoft MS-CHAP v2.

15 15. The implementation of claim 9 further comprising an implementation for provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties.

16. The implementation of claim 15 wherein the implementation for provisioning a public/private key pair comprises and implementation for providing a server-side certificate in
20 accordance with Public Key Infrastructure (PKI).

17. A computer usable medium having computer readable program code embodied therein for enabling secure communication, the computer readable program code in a computer program product comprising:

instructions for communication between at least first and second parties;

5 instructions for establishing a secure tunnel between the at least first and second parties using an encryption algorithm;

instructions for authenticating between the at least first and second parties over the secured tunnel; and

10 instructions for provisioning secure credentials between the at least first and second parties.

18. The computer program product of claim 17 wherein the instructions for communication between the at least first and second parties comprise instructions for a wireless implementation.

15

19. The computer program product of claim 17 wherein the encryption algorithm is a symmetric encryption algorithm.

20. The computer program product of claim 19 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.

21. The computer program product of claim 19 wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange.

22. The computer program product of claim 17 wherein the instructions for authenticating comprise Microsoft MS-CHAP v2.

23. The computer program product of claim 17 further comprising instructions for provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties.

24. The computer program product of claim 17 wherein the instructions for provisioning a public/private key pair comprise instructions for providing a server-side certificate in accordance with Public Key Infrastructure (PKI).